



**KNOXVILLE POLICE DEPARTMENT
KNOXVILLE, TENNESSEE**



Standard Operating Procedure – Real-Time Information Center (RTIC)

Subject: Real-Time Information Center SOP	Effective Date: April 9, 2026	Revised Date: May 6, 2026	Pages: 15
Cross Reference: General Order 4.24	Chief of Police Approval:		

Purpose

The purpose of this policy is to define the functions, duties, responsibilities, and operational guidelines for the RTIC and its personnel, while ensuring operations are conducted in a manner that upholds constitutional protections, privacy rights, and community trust.

Table of Contents

Purpose and Mission..... 3

Policy..... 3

Definitions..... 4

Personnel Assignment and Responsibilities 4

 RTIC Commander 4

 RTIC Supervisor 5

 RTIC Specialist 5

Training Requirements..... 6

Security of RTIC Space..... 6

Operational Procedures..... 7

 Hours of Operation 7

 Dispatch Deconfliction and Communications..... 7

 Call Prioritization..... 7

 Call for Service Response 8

 Requests from Field Personnel 8

 Virtual Patrolling 9

 Automated License Plate Recognition (LPR/ALPR) 9

Follow-Up Investigations and Requests for Information	9
Open-Source Intelligence (OSINT)	10
Special Events and Crowd Monitoring	10
Documentation	10
Drone as First Responder (DFR)	11
Tactical Operations Center (TOC) Integration	11
Camera Governance and Placement	12
Knoxville Police Department Owned Cameras	12
Mobile Camera Trailers.....	12
Integrated Cameras – Knoxville Connect (Community Camera Integration)	13
Video Retention and Data Storage	13
Open Records.....	14
Appendix A – Camera Retention Schedule	15

Purpose and Mission

1. The Knoxville Police Department's Real-Time Information Center (RTIC) shall operate as a centralized technology and intelligence support unit designed to enhance situational awareness, officer safety, and community protection through the responsible integration of advanced technology and real-time data systems. By providing timely and actionable intelligence, the RTIC supports informed decision-making, proactive policing, and effective incident response.
2. The Real-Time Information Center (RTIC) plays a critical role in delivering accurate, up-to-date information and enhancing situational awareness. Through proactive monitoring of available resources, the RTIC supports crime prevention and helps assess ongoing events to determine the need for additional deployment.

Policy

3. All RTIC operations shall comply with applicable federal, state, and local laws as well as Department policies. Personnel shall respect constitutional protections, including the First and Fourth Amendments, in all aspects of their duties.
4. The Knoxville Police Department and the RTIC are committed to respecting the reasonable expectation of privacy for all citizens and ensuring that the use of technology aligns with constitutional protections and community trust.
5. The use of facial recognition technology in conjunction with RTIC systems is prohibited. Evidence lawfully obtained through RTIC systems may be utilized by Department personnel in accordance with General Order 4.24.
6. The RTIC shall not collect, retain, or disseminate information about individuals or groups based solely on race, ethnicity, religion, gender, political beliefs, or other protected characteristics, except when such descriptors are part of a specific, credible suspect description or relevant investigative information.
7. All RTIC system access shall be logged and subject to audit. Any suspected misuse, including unauthorized access, inappropriate queries, or use of technology without a legitimate law enforcement purpose, shall be documented and reported through the appropriate chain of command. Misuse may result in further administrative review and disciplinary action in accordance with Department policy.
8. All personnel assigned to or operating in the RTIC are expected to maintain strict confidentiality regarding all observations, communications, and case-related information encountered within the Center. This includes discussions with officers, detectives, and any details pertaining to active or past investigations.

Definitions

9. Camera Feeds – Video utilized by the RTIC supplied from Department-owned cameras or voluntarily shared by public or private entities.
10. Drone as First Responder (DFR) – A program in which trained RTIC personnel pilot unmanned aircraft systems (UAS) to provide real-time aerial support to incidents.
11. Evidence.com – The web-based digital evidence management platform used by the Knoxville Police Department (also referred to as Axon Evidence.com).
12. Fusus /Axon Fusus – The authorized software platform and associated hardware (Core device) that connects camera networks to the RTIC and serves as the primary system for real-time monitoring.
13. Knoxville Connect – Community Camera Integration – A voluntary program through which private entities or individuals share access to their public-area-facing camera feeds with the RTIC.
14. License Plate Reader (LPR) / Automated License Plate Recognition (ALPR) – An automated camera-based system that captures and converts vehicle license plate data into searchable alphanumeric information and compares it against law enforcement databases. LPR is governed by a separate standalone Department policy.
15. Real-Time Information Center (RTIC) – A centralized law enforcement technology center, located at the Knoxville Public Safety Complex and operated by members of the Knoxville Police Department, that integrates information and technology resources to support field and investigative operations in real time.
16. RTIC Cameras – Any camera owned, installed, and maintained by the Knoxville Police Department and assigned to the RTIC. This does not include cameras owned by other City departments (e.g., Traffic Engineering, Public Building Authority).

Personnel Assignment and Responsibilities

17. Only personnel who have been approved by the Chief of Police or designee and who have completed required training are authorized to access RTIC systems. The RTIC operates under the Special Services Division of the Field Operations Bureau.

RTIC Commander

18. The Special Services Division Captain serves as the RTIC Commander and is responsible for the overall management, strategic direction, and compliance of RTIC operations. Duties include, but are not limited to:
 - a. Administering system access and establishing role-based permissions consistent with operational needs.

- b. Approving video sources integrated into the RTIC and authorizing non-evidentiary video retention when appropriate.
- c. Maintaining an accurate catalog of all RTIC-owned and partner camera feeds, including installation dates, locations, and maintenance history.
- d. Ensuring compliance with all applicable laws, Department policies, CJIS requirements, and privacy protections.
- e. Maintaining open communication with Department bureaus and partner agencies.
- f. Staying informed on emerging technologies and industry best practices to ensure the RTIC remains effective and current.
- g. Producing required reports detailing RTIC activity as directed by the Field Operations Deputy Chief.
- h. Plan and coordinate training for all RTIC staff.

RTIC Supervisor

19. The RTIC Supervisor is a sworn or professional staff position that is responsible for daily oversight of RTIC operations and personnel. In the absence of an RTIC Supervisor, the RTIC Commander will assume those responsibilities. Duties include, but are not limited to:

- a. Providing daily leadership, scheduling, and supervision of RTIC staff.
- b. Assigning and reviewing casework, ensuring timely completion of requests.
- c. Maintaining an accurate and current log of all camera feeds available to the RTIC.
- d. Reviewing and approving all requests for information or video footage submitted to the RTIC.
- e. Conducting documented, random audits of Specialist activity on a quarterly basis, including camera usage, LPR queries, DFR operations, and evidence uploads, to ensure compliance with policy, CJIS requirements, and privacy protections.
- f. Ensuring all RTIC activities comply with Department policy, CJIS requirements, and applicable laws.
- g. Filling the duties of an RTIC Specialist as needed to support shift coverage or to enhance operational support.
- h. Limiting distractions in the RTIC to allow full attention to cameras and assignments.

RTIC Specialist

20. RTIC Specialists (also known as RTIC Operators) are sworn or professional staff positions that are responsible for the core operational activities of the RTIC. Duties include, but are not limited to:

- a. Monitoring active calls for service and providing real-time intelligence to field personnel through authorized communication channels.

- b. Providing analytical and investigative support for criminal incidents that have already occurred, when such support is requested and approved by the RTIC Supervisor or Commander.
- c. Conducting proactive virtual patrolling of camera feeds for criminal activity, suspicious behavior, and public safety concerns.
- d. Monitoring police radio, CAD, LPR systems, open-source intelligence, and other available data sources.
- e. Assisting with investigations using RTIC systems and resources, including review of historical camera footage and records.
- f. Monitoring major incidents, special events, and weather conditions that may impact public safety.
- g. Supporting other City departments when such assistance aligns with Department policies.
- h. Maintaining a daily activity log documenting calls monitored, cameras accessed, requests fulfilled, and significant intelligence provided.
- i. If properly trained and certified, piloting unmanned aircraft systems as part of the DFR program.
- j. Providing court testimony as required regarding actions taken, information obtained, and systems utilized.

Training Requirements

- 21. All personnel assigned to the RTIC shall complete initial training that includes:
 - a. Constitutional law, with a focus on reasonable expectation of privacy.
 - b. Department policies and RTIC operational procedures.
 - c. RTIC technology systems and equipment, including Axon Fusus and other platforms.
 - d. Criminal Justice Information Services (CJIS) compliance requirements.
- 22. Ongoing training shall be provided to ensure personnel remain current with legal updates, technological advancements, and evolving best practices, including changes in applicable laws and emerging trends in real-time information center operations.

Security of RTIC Space

- 23. Access to the RTIC workspace shall be controlled. Only authorized personnel shall be granted keycard access. All other visitors must be escorted or supervised by RTIC personnel and must be pre-authorized by the RTIC Supervisor.
- 24. Tours of the Center may be provided by staff but must first be approved by the RTIC Commander.

Operational Procedures

Hours of Operation

25. Hours of operation for the RTIC will be recommended by the RTIC Commander and approved by the Field Operations Deputy Chief, based on staffing levels, current crime trends, special events, and other relevant operational factors.
26. In the event of a significant incident outside of operational hours, the RTIC Supervisor shall be contacted to determine if callback is necessary. A callback rotation shall be maintained based on the number of personnel assigned and current staffing levels. An RTIC or Special Services Division supervisor on call will determine whether a callback response is warranted.

Dispatch Deconfliction and Communications

27. RTIC personnel shall maintain communication through authorized radio channels, CAD, and telephone systems. The designated RTIC radio call sign is "700." Each Specialist will also be assigned an individual call sign in the 700 series (e.g., 700, 701, 702). The designated CAD identifier for monitoring purposes is KP_RTIC700; individual staff shall log in using their assigned individual CAD credentials for accountability.
28. RTIC Specialists shall not relay information via radio, CAD, or telephone prior to a call being assigned by Dispatch, unless there is an articulable and immediate threat to public safety. Once Dispatch has assigned officers, Specialists may begin relaying relevant support information.
29. If an RTIC Specialist observes an incident requiring a police response, they shall immediately contact Dispatch via radio or phone, providing the location, description of what is occurring, and identifying details. Specialists shall not contact field officers directly unless there is an articulable and immediate threat to public safety or a time-sensitive LPR alert warrants direct contact (see LPR section). RTIC staff shall not assume Dispatcher duties unless explicitly authorized by supervisors of both the RTIC and Dispatch.

Call Prioritization

30. Calls for service shall be prioritized using the following structured approach:
 - a. Priority One calls shall receive the highest level of attention. RTIC personnel shall immediately begin monitoring all available resources at the incident location and shall continue working the event until it is stabilized or no additional actionable intelligence can be developed.
 - b. Priority Two calls shall be monitored as resources allow, with personnel evaluating each call as information is received from dispatch to determine whether RTIC resources can provide meaningful intelligence.

- c. Priority Three and Four calls shall be reviewed as time permits, with personnel assessing whether actionable information can be developed and provided to responding officers prior to arrival.
- d. Active priority calls take precedence over non-priority calls awaiting review.

Call for Service Response

31. At the beginning of each shift, RTIC staff shall conduct a Camera Function Evaluation. This is a check of camera feeds, positioning, and proper functioning. Any issues shall be documented in the Daily Activity Log. When a camera feed is down, the Specialist shall notify the RTIC Supervisor, notify the appropriate camera custodian, and conduct regular follow-up until the camera is restored.
32. When monitoring a call for service, RTIC personnel shall:
- a. Immediately access available cameras in the vicinity and begin monitoring activity.
 - b. Monitor associated CAD comments and radio traffic.
 - c. Request that Dispatch add RTIC to the call.
 - d. Provide actionable information, such as: live camera observations, updated suspect/scene information, relevant historical reports, or crime data – to responding units or dispatchers.
 - e. Search relevant records management systems for information related to the incident.
 - f. Document all actions taken and information provided in the Daily Activity Log.
33. Following resolution of an incident, RTIC personnel shall conduct a follow-up review of the location when appropriate to identify any return of suspects or continuation of activity. If additional concerns are identified, personnel shall notify Dispatch and request further response as necessary.
34. RTIC personnel shall continue monitoring incidents until no additional actionable intelligence is available. All information provided by the RTIC, including video footage and still images, is intended as an investigative lead and shall not be considered a source of positive identification. Responsibility for verifying information and determining appropriate enforcement action remains with the assigned officer or detective.

Requests from Field Personnel

35. Officers or detectives requiring RTIC assistance may contact the RTIC by:
- a. Telephone or
 - b. Contacting a member of the RTIC on the appropriate radio channel using the call sign "700".
36. RTIC Specialists shall actively monitor the KPD channels at all times during operational hours to ensure timely response.

Virtual Patrolling

37. As time allows, RTIC staff may cycle through available camera feeds, actively observing for potential incidents or suspicious activity. Priority areas may be selected based on recent crime trends or actionable intelligence.
38. When RTIC personnel observe suspected or actual criminal activity on camera, they shall notify Dispatch via the appropriate radio channel and request creation of a call for service. The RTIC serves as the complainant in these cases and does not dispatch officers directly.
39. Once dispatch assigns an officer to the call, RTIC staff will follow their normal procedures, as described above.

Automated License Plate Recognition (LPR/ALPR)

40. ALPR/LPR is an integral component of RTIC operations and is governed by a separate standalone Department policy. RTIC Specialists shall actively monitor ALPR alerts and respond appropriately to notifications generated by the system.
41. Specialists may directly contact officers in the field regarding time-sensitive LPR alerts when a license plate match is visually confirmed, vehicle description and direction of travel are verified, and an officer is confirmed to be in the vicinity and able to respond in a timely manner. Immediately following direct notification, the Specialist must ensure that Dispatch has received and acknowledged the information.

Follow-Up Investigations and Requests for Information

42. RTIC personnel are available to support ongoing investigations through review of historical data upon request from investigating officers or detectives. All requests for information or video footage must be submitted in writing to the RTIC Supervisor for review and approval. Requests must include:
 - a. Report number.
 - b. Type and nature of the investigation.
 - c. Relevant details to assist with data retrieval: date, time, location, and descriptions of individuals, vehicles, or events.
43. If a request is time-sensitive, an initial verbal request may be made, but it must be followed promptly by email to ensure proper documentation. All requests shall be reviewed and approved by an RTIC Supervisor prior to assignment. The Supervisor may approve, deny, or request modifications.
44. The assigned Specialist shall document the following when responding to a request:
 - a. name of Specialist,
 - b. date and time of review,
 - c. timestamp(s) of footage,
 - d. camera location and orientation,

- e. video file or screenshot,
- f. and a summary of the video content.

45. Relevant footage shall be uploaded to Evidence.com and assigned to the requesting officer.

Open-Source Intelligence (OSINT)

46. RTIC personnel may monitor publicly available, open-source intelligence related to planned or ongoing special events, large gatherings, or incidents that may impact public safety. This monitoring shall be limited to publicly accessible sources and conducted for the purpose of enhancing situational awareness, identifying safety concerns, and supporting operational planning.

47. OSINT monitoring shall not include circumventing privacy settings, accessing restricted accounts, or engaging in deceptive practices to obtain information. RTIC personnel shall not engage in monitoring individuals or groups solely based on their exercise of constitutional rights.

48. Information identified through OSINT that may impact public safety shall be communicated to appropriate personnel. Information gathered shall not be retained beyond its operational usefulness unless it becomes part of an active investigation or official report.

Special Events and Crowd Monitoring

49. Special events include sporting events, festivals, concerts, parades, and other public gatherings. The RTIC shall use available technological resources to monitor for suspicious activity both before and during events. Relevant findings shall be reported to appropriate personnel as soon as practicable.

50. RTIC staff shall provide situational awareness updates regarding events and surrounding activities to Special Event Supervisors. Special Event Supervisors should be present with or in communication with RTIC personnel during major events.

Documentation

51. RTIC Specialists shall maintain a daily activity log documenting calls for service monitored, cameras accessed, LPR queries, DFR deployments, requests fulfilled, and significant intelligence provided to field personnel. This log ensures accountability, continuity of operations, and the ability to review RTIC contributions to incidents.

52. Relevant information provided by RTIC shall be documented in appropriate logs and incident or crime reports.

Drone as First Responder (DFR)

53. RTIC personnel assigned and certified to operate unmanned aircraft systems (UAS) may deploy drones to support calls for service, enhance situational awareness, and provide real-time intelligence to field personnel. DFR operations shall be conducted in accordance with Federal Aviation Administration (FAA) regulations, Department policy, and all applicable laws.
54. DFR deployments shall be primarily tied to active calls for service, critical incidents, or situations where aerial perspective can improve officer safety or incident resolution. Priority shall be given to incidents involving potential threats to life or safety, fleeing suspects, missing persons searches, or situations where real-time aerial intelligence may significantly impact outcomes.
55. Prior to deployment, RTIC personnel shall evaluate the necessity of drone use based on call type, location, airspace considerations, weather conditions, drone airworthiness, and available resources. When deployed, personnel shall maintain communication with responding officers and Dispatch, providing real-time updates including suspect movement, scene conditions, hazards, and other relevant intelligence.
56. DFR operations shall minimize intrusion and be consistent with constitutional protections. RTIC personnel shall not utilize drones for random surveillance or to monitor individuals or groups absent a legitimate law enforcement purpose tied to a specific incident, public safety concern, or authorized operation.
57. All DFR deployments shall be documented in the daily activity log. Video or data with evidentiary value shall be uploaded to Evidence.com. RTIC Supervisors shall review a sampling of drone deployments to ensure proper justification, appropriate use, and compliance with operational guidelines, including review of flight logs and associated calls for service.
58. All DFR deployments shall be documented on a publicly accessible dashboard to promote transparency and community awareness. The dashboard shall provide general information regarding deployments, including the type of call for service the DFR assisted with, while ensuring any sensitive or legally protected information is not disclosed.

Tactical Operations Center (TOC) Integration

59. The RTIC shall serve as the Department's Tactical Operations Center (TOC) when activated during critical incidents, severe weather events, large-scale public gatherings, or other situations requiring coordinated command and control. Sharing this space eliminates duplication of staffing and resources while allowing the RTIC to provide critical situational awareness in support of TOC operations.

60. Personnel assigned to operate within the TOC during activation shall sign in upon entry, maintain an ICS 214 Activity Log, and operate within the established Incident Command System (ICS) structure. All personnel shall adhere to assigned roles and responsibilities to ensure efficient and coordinated incident management.
61. All technology and available resources within the TOC shall be operated only by RTIC personnel assigned to support TOC operations. This is to ensure systems are utilized by personnel with the appropriate training and authorized access.
62. An RTIC staff member shall be present during all TOC activations. The staffing schedule for TOC operations shall be coordinated by the RTIC Supervisor and approved by the RTIC Commander.

Camera Governance and Placement

Knoxville Police Department Owned Cameras

63. All Knoxville Police Department owned camera will be operated by the RTIC staff and in a manner that respects individual privacy rights. Cameras will never be installed in locations where there is a reasonable expectation of privacy.
64. RTIC-managed camera placement shall be determined through a data-driven process that includes review of multi-year calls for service data and crime trends, input from Department personnel and community members, and evaluation of infrastructure availability. Final approval for camera placement shall be made by the Chief of Police or designee.
65. All RTIC-managed cameras shall be overt and clearly marked to identify their association with the Knoxville Police Department. Cameras shall only be installed in locations where proper authorization has been obtained and where there is no reasonable expectation of privacy.
66. Camera placements shall be reviewed regularly to ensure continued effectiveness and alignment with current crime patterns and operational needs. An updated list of fixed RTIC-managed camera locations shall be maintained on the Department's public website to support transparency.

Mobile Camera Trailers

67. Mobile camera trailers shall be tracked and maintained by RTIC personnel to ensure accountability and operational readiness. Units shall be clearly marked as Knoxville Police Department equipment.
68. Placement of mobile camera trailers requires approval of the RTIC Commander.

69. Mobile camera locations do not need to be posted on the Department's website due to their frequent relocation. Use of mobile cameras shall be temporary and shall never be deployed in a covert manner.

Integrated Cameras – Knoxville Connect (Community Camera Integration)

70. The Knoxville Police Department maintains a voluntary Community Camera Integration program (Knoxville Connect) through which businesses and residents may share access to their security cameras to assist in criminal investigations. Participation may occur through Registry (sharing location only) or Integration (providing live or recorded access via the Fusus platform).

71. Access to Integrated Cameras shall be used solely for legitimate law enforcement purposes and in accordance with applicable agreements and policies. RTIC staff may monitor Integrated Cameras when related to an active call for service, investigation, system audit, or approved training. These permissions are granted by the camera owner and may be revoked at any time.

72. The RTIC shall not continuously record or store live feeds from Integrated Cameras. When footage is downloaded for a law enforcement incident, it shall be stored on KPD systems in accordance with applicable state laws and Department policy. After any incident where camera access directly supported police action, the RTIC Supervisor shall notify the camera owner with a summary of the event.

73. Responsibilities of camera owners include: purchasing any required integration equipment (e.g., Fusus Core devices); managing public or media inquiries related to their cameras; retaining ownership of all video content; and managing camera purchase, repair, and operation. All video obtained from Integrated Cameras remains the property of the contributing entity.

74. During RTIC operational hours, only RTIC personnel, or the camera owner if the camera is not RTIC-owned, are permitted to manipulate or control camera systems. Outside of operational hours, permission to operate cameras may be granted by the RTIC Commander.

Video Retention and Data Storage

75. All video retention associated with RTIC systems shall comply with applicable laws, including the Knoxville City Code and the Municipal Technical Advisory Service Police Records Schedule pursuant to T.C.A. § 10-7-702, as well as Department policy.

76. Unless video is identified as having evidentiary or training value, it shall not be retained beyond thirty (30) days. When video is determined to have evidentiary value, it shall be uploaded to Evidence.com and retained in accordance with applicable laws and Department policy governing digital evidence. Evidence.com maintains an audit log that

includes the associated complaint number and the identities of any personnel who access or retrieve the evidence.

77. Non-evidentiary retention beyond 30 days requires a documented request and approval from the RTIC Commander. Eligible examples include footage used for training, potential civil liability involving the City of Knoxville, or footage related solely to Department operations.
78. Ongoing storage must occur on a secure, City-approved video management system compatible with RTIC cameras and approved by the City of Knoxville Information Technology Department.
79. Retention periods may vary depending on the source of the video, including RTIC stationary cameras, mobile camera trailers, unmanned aircraft systems, and externally owned camera systems. These retention guidelines are outlined in Appendix A and shall be followed accordingly.
80. All data obtained and stored by the RTIC shall be used solely for legitimate law enforcement purposes. Access to stored images and footage is restricted to authorized personnel.

Open Records

81. The release of images is subject to all applicable open records laws; requests for copies must be submitted in accordance with state law the Knoxville City Code and Administrative Rules, and current Department policy. Requests from outside KPD personnel or through legal process (e.g., FOIA, subpoena) must be submitted in accordance with KPD open records policies and procedures.

Appendix A – Camera Retention Schedule

The following retention guidelines apply to video recorded by RTIC-managed or integrated systems. Retention periods are subject to applicable state law and Department policy. Video with confirmed evidentiary value shall be uploaded to Evidence.com regardless of the source.

Video Source	Standard Retention	Extended Retention	Notes
RTIC Stationary Cameras	30 days	Per Evidence.com policy	Evidentiary video must be uploaded to Evidence.com
Mobile Camera Trailers	30 days	Per Evidence.com policy	Evidentiary video must be uploaded to Evidence.com
UAV	15 days	Per Evidence.com policy	Evidentiary video must be uploaded to Evidence.com
License Plate Readers	30 days	Per Evidence.com policy	Evidentiary video must be uploaded to Evidence.com.
Other City Department Cameras	30 days	Other City Department Policies	Evidentiary video must be uploaded to Evidence.com
Integrated/Donor Cameras (Knoxville Connect)	Per owner agreement	Per owner agreement	Owner retains ownership; RTIC may download for active incidents. Any video retained must be downloaded to Evidence.com

**Non-evidentiary extended retention (training, civil liability, or Department operations) requires documented request and RTIC Commander approval.*